

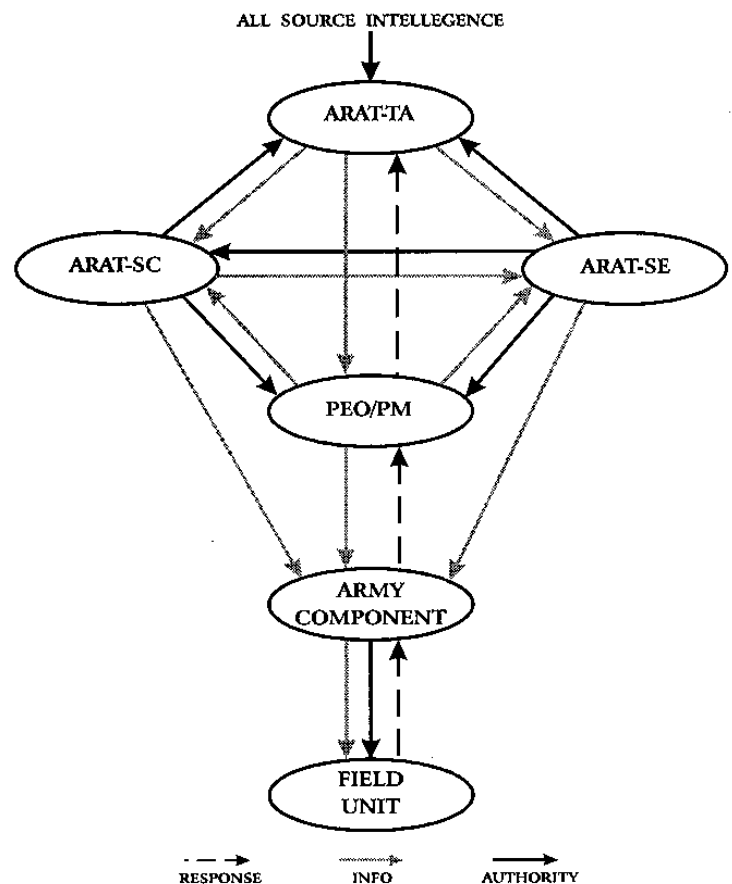


## Volume 1, Issue 3

October 1994

# ARMY RAPID REPROGRAMMING ARCHITECTURE: Meeting The Challenges of Technology & Information Warfare

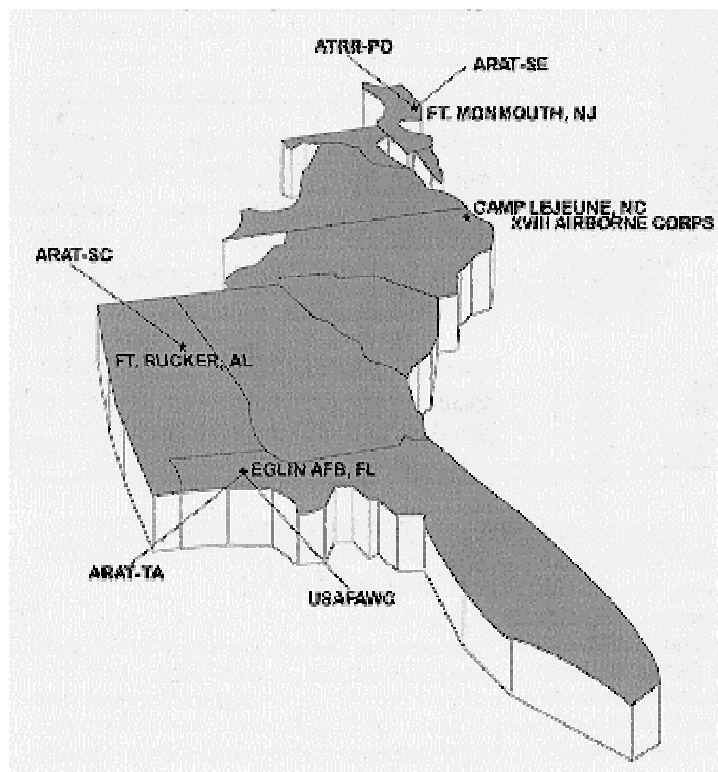
BRAVE BYTE '94	Page 1
MULTISERVICE REPROGRAMMING	Page 1
INFORMATION OPERATIONS	Page 2
MESSAGE FORMATTING (Part 2)	Page 4
JULLS (Part 2)	Page 5
ONE LAST LOOK	Page 6
ARAT BBS (Part 2) E-MAIL	Page 6
PUMP UP THE VOLUME	Page 7



---

## ***BRAVE BYTE 94 PROVES A SUCCESS FOR ARAT!***

The U.S. Army held its annual reprogramming exercise, BRAVE BYTE 94 recently from 23 April to 6 May 94 throughout the eastern United States (see figure below). The Army conducted BRAVE BYTE 94 together with the newly-formed U.S. Atlantic Command's exercise, AGILE PROVIDER 94. These exercises successfully tested the ability of the Army reprogramming community to rapidly reprogram two specific radar warning receivers in a simulated contingency environment. Key Army participants included the XVIII Airborne Corps, deployed to Camp Lejeune, NC, the ARAT-TA, at Eglin AFB, FL, the ARAT-SE center at Fort Monmouth, NJ, the ARAT-SC at Fort Rucker, AL and the ATRR-PO at Fort Monmouth, NJ. In addition, the USAFAWC at Eglin AFB provided analytical support.



BRAVE BYTE 94 had five primary objectives: exercise the interaction of ARAT-TA with supported/supporting commands and agencies; evaluate the capability of the ARAT Bulletin Board System (BBS) to exchange near-real time technical and operational data; evaluate the ARAT Local Area Network (LAN) capacity to process information during contingency operations; decide the utility of draft message format templates; and evaluate ARAT technical awareness training. The entire reprogramming process was exercised except for software change uploading to fielded systems.

This exercise achieved some milestones in U.S. Army reprogramming history. The ARAT BBS was used for the first time to pass information between Army units. The BBS provided a vital link for the reprogramming process throughout the exercise. Formats for message templates (such as Threat Impact Message, Reprogramming Impact Message, etc.) were tested for the first time in message transmission to the appropriate recipients. Much knowledge was learned about the utility of

these templates and their possible, future incorporation into the Army reprogramming effort.

BRAVE BYTE 94 provided twenty-six lessons learned. These were documented in a formal After Action Report (AAR), using the Joint Universal Lessons Learned System (JULLS) formats. Lessons learned focused on the ARAT BBS (8 lessons learned), message formats (5), reprogramming procedural requirements (6), reprogramming tools (3), training (2), and ARAT-TA operations (2).

Many of these problem areas are now being addressed. These include refining BBS operations to better support field users, and a staffing study to identify personnel requirements at the ARAT-TA. A forum will be held in the future to address issues that require long-term solutions. Initial distribution of the BRAVE BYTE 94 AAR/Lessons Learned was made in early July. Any agency not on the initial distribution list should contact Mr. Sok Kim, ATRR Project Officer to obtain a copy. He can be reached at DSN: 992-1337, Comm: (908) 532-1337, or by E-mail at [arat@ccmail.sed.monmouth.army.mil](mailto:arat@ccmail.sed.monmouth.army.mil). POCs are Mr. Ken Kragh/Mr. Joe Skarbowski, DSN: 992-6003.

---

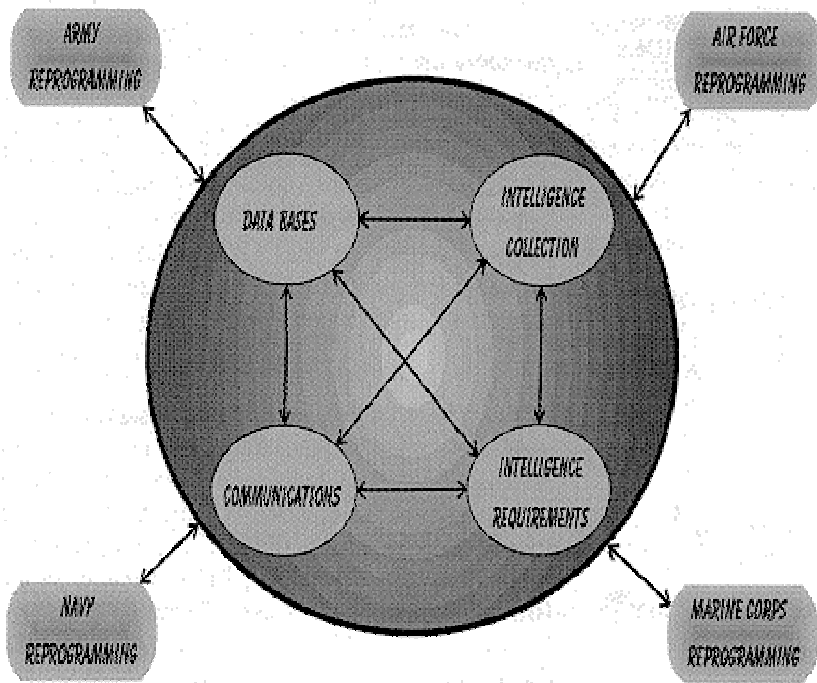
## **Multi-Service Reprogramming Study Underway**

During Operation Desert Storm, all services operated in the same electromagnetic environment. Each service, however, used different data and methods to produce reprogramming changes. A multi-service reprogramming study is underway to improve this situation and move the services closer to compliance with joint philosophy (see Figure next page). The study, when finished, will describe Electronic Warfare (EW) reprogramming tasks performed at each Reprogramming Center. In addition, this study will quantify where the services are, decide how to best standardize the process across all services, recommend improvements in the EWIR

**(continued on Page 2)**

## Multi-Service Reprogramming (continued)

Database, recommend communications improvements between all reprogramming operations, and establish intelligence requirements for the services.



## **Joint Service Reprogramming: Supporting Information Warfare**

A contractor study team was established to perform this work with a current expected completion date of February 1995. This study team will visit the services' reprogramming centers and several support agencies. These site visits will document the Unit Mission; System Engineers Tasks; Intelligence Analysts Tasks; and Computer/Communications Personnel Tasks. Documentation such as regulations, operating instructions, computer architecture, and system handbooks will also be examined. A joint service oversight team will monitor and direct the contractor. The United States Air Force Air Warfare Center (USAFAWC) provides daily monitoring of the contractor and helps resolve issues in accomplishing this study.

So far, the study team has visited several US Air Force sites and developed a description of their reprogramming operations. As a result, the services have agreed to write a Joint Operational Requirements Document (ORD) for EW reprogramming. Upcoming visits are scheduled for several US Navy sites and CECOM, Fort Monmouth, NJ (31 Oct - 4 Nov 94).

After these visits, process description documents will be written for the Navy and Army. These documents will include a Reprogramming center Overview, Command and Support Relationships and how they fit into the reprogramming process, the reprogramming process for the center, and operations/recommendations. The study team will use these documents

to develop a Joint Service Concept of Operations for Reprogramming and a Recommended Implementation Plan (for reprogramming center improvements over the next five years). These documents will serve as the basis of future reprogramming direction, if accepted.

This study provides a unique forum for the services to discuss multi-service reprogramming issues. The ultimate goal is to achieve the integration of all reprogramming actions throughout the military. Such a process could save money for all services by sharing equipment, communications, and data. POCs are LTC Bert Napoleon, DSN: 872-8899/CPT Clements, DSN: 872-2166.

---

**"ARAT BULLETIN" will be published quarterly and is intended to provide the ARAT community with current information. You are invited to submit input for improving this publication, or present articles which will be of interest to our readers. You may Fax correspondence to the Editor at (908) 532-5238. Include your name, telephone number, and source of information.**

---

## **Information Operations**

*"The nature of armies is determined by the nature of the civilization in which they exist."*

**B.H. Liddell Hart**

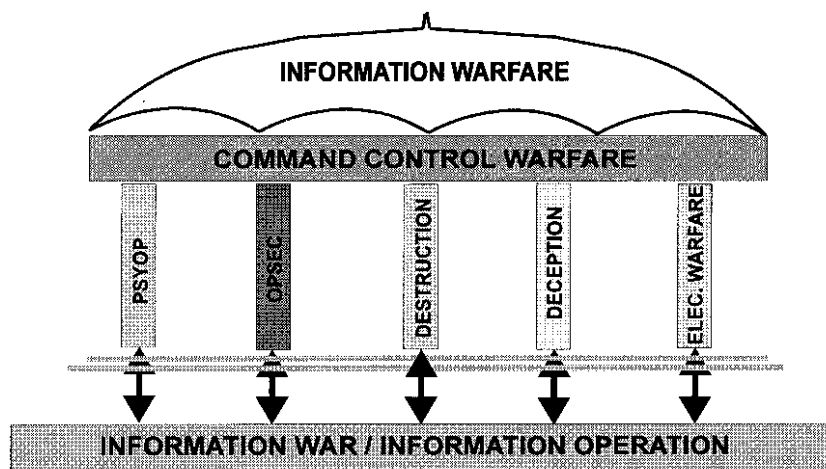
Information Operations (IO) identifies information as an essential enabler of military power at the strategic, operational, and tactical levels. Information age technologies serve to multiply the talent and potential of leaders and soldiers, thus contributing to friendly mission success in joint, multinational, and interagency operations. Weapons systems, using discrete information parameters, are more destructive, accurate, effective, and versatile to employ.

**(continued on Page 3)**

## Information Operations (continued)

Recently, Headquarters Department of Army leadership directed the publication of an Army concept and doctrine for carrying out DOD Policy for Information Warfare. The Training & Doctrine Command (TRADOC) has undertaken an accelerated schedule to produce Army doctrine. Using the Concept Based Requirements System (CBRS), a concept for Information Operations was written as a TRADOC Pamphlet, Series 525. As of this date, the publication is known as TRADOC Pam 525-XX.

The final draft concept (headed for publication) describes the importance of and how to win the information war in military operations from now into the twenty-first century. This concept defines information operations (IO) as the framework for integrated support for battle command and describes the operational capabilities necessary for its planning and execution. The proposed definition for information operations reads, "continuous operations that enable, enhance, and protect the commander's decision and execution cycle while influencing an opponent's. These are accomplished through effective intelligence, Command & Control (C2), and Command & Control Warfare (C2W) operations supported by all available friendly information systems. Information operations, supporting the battle command, are conducted throughout the full range of military operations."



The objective of IO is to enable, enhance, and protect the use of information in the friendly decision and execution process while influencing (degrading, controlling) an adversary's decisions and actions through manipulation of his information/ information system. In joint doctrine, the engagement of the adversary's information system is called C2W and includes electronic warfare (EW), operations security (OPSEC), military deception, psychological operations (PSYOP), and physical destruction. These five C2W pillars, guided by intelligence support, are used to employ counter C2 and C2-protect actions.

Commander's must visualize a battle space within which they will fight under more varied and ambiguous conditions than ever before. They must act swiftly to achieve decisive victory and minimize casualties. Critical elements to this success include having sufficient/relevant knowledge on ones precise location, knowing the location of other friendly forces, along with the strength, posture, location, and signature of the adversary's warfighting means. The possession of rudimentary facts about the adversary's disposition is no longer sufficient in this age of high

technology. Sophisticated C2 electronic protection means will allow the commander to maintain momentum, employ surprise, and conduct highly lethal high payoff attacks.

In response to emerging doctrine, the Vice chief of Staff approved the Intelligence & Security Command's initiative to establish an information operations center, dubbed the army C2W intelligence Cell (C2W-I Cell). The organization's cadre of personnel started August 15, 1994 under the leadership of COL Michael Tanksley. COL Tanksley previously served as the driving force behind the Joint Staff's publication of C2W policy found in JCS Memorandum of Policy 30 or MOP 30. The requirements for establishing the C2W Cell are: to provide synchronization of IO; coordinate intelligence and data base support; orchestrate human intelligence (HUMINT) support; and provide technical liaison support via electronic means with National Agencies, DOD, USAF, and USN IO activities. As the C2W-I Cell matures, functions are expected to be refined to meet user needs.

Action is currently underway within the C2W-I Cell, to transfer TRADOC's Army Reprogramming Analysis Team - Threat Analysis (ARAT-TA) activity to INSCOM. This will better align functional aspects of ARAT-TA with an Army organization experienced in conducting operations at strategic/theater level. The new organizational relationship is expected to improve threat analysis support to operational units which have discrete requirements for information. As the ARAT-TA evolves to support larger numbers of high technology target sensing systems, the INSCOM C2W-I Cell will provide a greater role in coordinating information/ intelligence support needs to planning elements engaged in military deception, electronic warfare, and physical destruction activities. The C2W-I Cell expects to support media, OPSEC, PSYOP, digitization, and sensor-to-shooter planning requirements as well.

Winning the information war is but one aspect of the Army's Modernization Strategy. Understanding it in warfighting terms to cause decisive victory will require new skills and tactics involving elements not commonly viewed as warfighting concerns. The doctrine being unveiled by TRADOC will help shape future Army battle command across the operational continuum. POCs are Major (P) Karen McManus, DSN: 235-2477, Sok Kim/Dan Hearn, DSN: 992-1337.

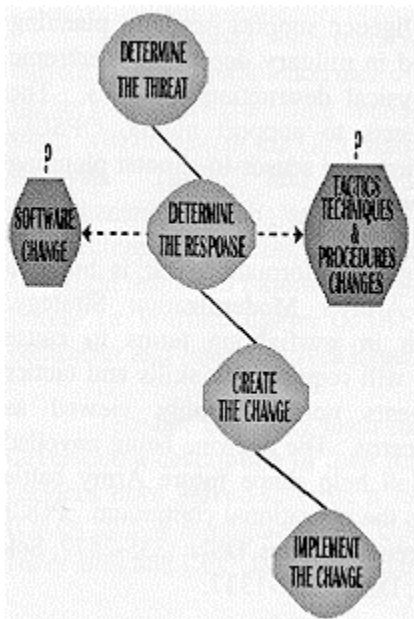
## MESSAGE FORMATTING: DATA DISTRIBUTION TO FIELDDED ATSS (Part 2 in a Series)

Part 1, (ARAT BULLETIN, July 1994), introduced message formatting and discussed Army efforts to develop standardized formats. Part 2 examines the process of data distribution and how it is affected by message formats.

EW systems exploit radiated signals by measuring different emitter parameters and comparing them with those of known radar systems. What is critical to optimum system performance, is the internal database library of enemy and friendly radar parameters. The library must be complete, accurate, and up to date to simplify emitter identification. This completed data requires the coordinated efforts of many agencies. The support facilities must identify threat changes and respond rapidly to support requests from deployed units. Consequently, a responsive resource distribution system is critical.

A primary concern is the identification of the communications network for rapid reprogramming data distribution. Network plans must identify: communication links to all potential theaters, new communications equipment, and priority use of existing networks. They must also provide accommodations to meet worldwide contingencies and establishment of specialized message formats. Message formats and the communications network must be compatible.

It is possible that future rapid reprogramming will involve two-way transactions between the ARAT-SE/SC's and Outside Continental United States (OCONUS) users. The process is initiated with the transmittal of a Threat Change Validation Request (TCVR), asking for support and collection priority. Other messages, their functions, and how they link the reprogramming community are identified within the four reprogramming process steps (see diagram below).



### Determine the Threat

Designated national, theater, and tactical assets collect and process signature data that could be provided in a timely manner to an Intermediate Processing Center (IPC) (located in the theater or CONUS) for threat validation. After analysis, the IPC could transmit a Threat Change Validation Message (TCVM) consisting of validated signature data to the ARAT-TA and Scientific & Technical Intelligence (S&TI) centers. The TCVM could be initiated by the IPC or in response to the TCVR.

### Determine the Response

On receipt of the TCVM, ARAT-TA could provide the PM, ARAT-SE, and ARAT-SC with early threat change indications and coordinate an impact analysis for the affected Army TSS. If a change in software is warranted,

the supporting ARAT-SE could issue a Threat Impact Message (TIM) to the operational users, assessing the impact of this threat to the affected TSS.

### Create the Change

When a software change is warranted, the ARAT-SE would analyze potential software solutions. The ARAT-SE would inform the theater Commander in Chief (CINC/IPC), ARAT-TA, PM, ARAT-SC, and users of the proposed reprogramming solution and implementation schedule by issuing a Reprogramming Impact Message (RIM). The operations impact, coupled with the software impact information to the PM and theater commands, gives a complete picture of the EW environment and the field commander's ability to operate within that environment. Ultimately, it is his decision reflected in either a Software Change Request (SCR) (a request to forward software updates within the timetable described in the RIM) or an Operational Change Request (OCR) (notification to implement a desired change in hardware or TTP alternatives). After creation of the software change package, the ARAT-SE issues it as a Software Change Message (SCM).

### Implement the Change

The SCM is distributed electronically to the theater field commander. This commander gives the final installation authorization to affected units by an Implementation Message (IMP). Data transfers might include extensive files of information and should be accomplished by a system that provides reliability and speed. Secure data communication resources should be available to all software reprogramming agencies.

The coordination of all events comprising this process requires rapid exchange of classified data between many geographically dispersed sites. This assures that new information is verified and equipment is quickly updated with the most current information. Reliance on normal Army channels for the rapid, two-way communications necessary to implement rapid reprogramming will probably be insufficient to meet future battle requirements and the time constraints of AR 525-15.

The ATRR-PO is establishing a message format working group to address the required message formats and to formulate and recommend rapid reprogramming message format standards for the Army, including, 1) definition of message types, 2) establishment of methodology for communicating the messages, and 3) approval of the data format.

(continued on Page 5)

---

## Data Distribution (continued)

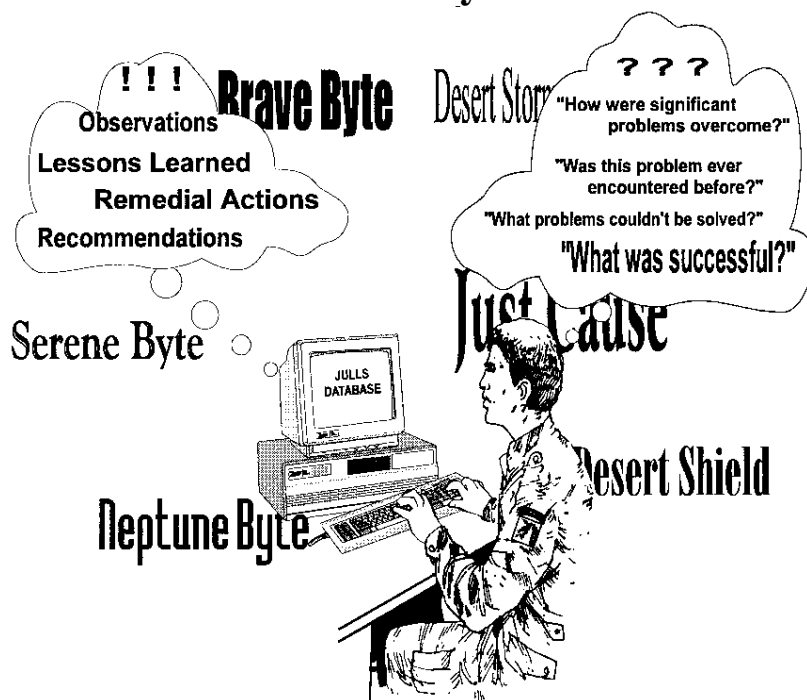
Once these standards are in place, our commanders can fully exploit the technological superiority of their equipment. POCs are Mr. Ken Kragh/Mr. Gary Parker, DSN: 992-6003.

---

# JULLS: BETTERING THE FUTURE BY BUILDING ON THE PAST (Part 2 in a Series)

*"An invasion of armies can be resisted, but not an idea whose time has come."*  
Victor Hugo

## Joint Universal Lessons Learned System



Part 1, (ARAT BULLETIN, July 1994), discussed the Joint Universal Lessons Learned System (JULLS), purpose, and associated data base. Part 2 examines the mandatory section.

JULLS has a rigidly-structured, unique format which is particular to it. We find in Joint Publication 1-03.30 that JULLS "enables After

Action Reports (AAR) to be more efficiently categorized, managed and accessed." JULLS is designed to accomplish the objectives set forth in this publication through the use of data entry fields. These fields require specific information for all lessons learned which provides commonality across any JULLS submissions. A JULLS submission is comprised of the narration or mandatory section (discussed here) and the Remedial Action Management Program.

The mandatory section contains numerous data entry fields. Certain fields must be manually filled in. Some fields can be filled in manually or not (your option), while still others are filled in by the application itself. There are ten key fields in this section which comprise about 95% of the mandatory section. These are Lessons Learned, Keywords, JULLS Number, Point-of-Contact, Exercise, Title, Observation, Discussion, Recommended Action, and Comments, of which the first two are briefly discussed.

The Lessons Learned field is the key part of the JULLS. This field lets you explain how to solve or work around the problem. You should submit a lessons learned regardless of whether or not there was a solution. (Someone else might be able to solve the problem.)

The Keywords field is probably the second most important part. These words allow quick retrieval of specific files from the JULLS data base. They can be determined and assigned by the originator. However, it is recommended that they be taken from the Joint Exercise Management Package (JEMP), Automated Keywording System (JAKS) computer program associated with JULLS. This allows all users to employ common keywords which aid database queries. The Army (Target Sensing Systems) Rapid Reprogramming Project Office (ATRR-PO) has requested the next version of JAKS list "reprogramming" as a keyword.

The information in these fields must be as accurate as possible. Accuracy results in a ready-to-access library of military information, as well as your observations and ideas which keep the ARAT effort going. Our future depends on what we do today and how we apply it tomorrow. Part 3 will discuss the Remedial Action Management Program and also, explore the future of Army and ARAT lessons learned. POCs are Mr. Sok Kim/Mr. Joe Skarbowski, DSN: 992-1337.

---

---

# ONE LAST LOOK

*by Stephen M. Hardy*

*The following article is an excerpt from the original story, published in Journal of Electronic Defense, June, 1994. Reprinted by permission of the Journal of Electronic Defense, Horizon House Publications, Inc. The Journal of Electronic Defense is the publication of the Association of Old Crows.*

Colonel Thomas Reinkober, outgoing project manager for aircraft survivability equipment (ASE) at the SFAE-AV-AEC offices in St. Louis, MO, has been very influential in the renaissance of Army Electronic Warfare (EW). He has overseen initiation of several Army EW's most advanced programs during his four-year tenure. Two programs include the Advanced Threat Infrared Countermeasures (ATIRCM) and Advanced Threat Radar Jammer (ATRJ) systems. These programs, in particular, represent Army aviation's most recent EW masterworks. They work in tandem and enable helicopters to operate with confidence in a multispectral threat environment.

The ATIRCM system combines missile warning with directable infrared radiation (IR) countermeasures in a single package. There are four missile warning sensors mounted on each platform. When the sensors detect an incoming missile, the system automatically slews the ATIRCM jamming head in the direction of the threat. A missile tracker on the jam head further refines the direction of the jamming transmission to within milliradians of the missile's flight path for optimal countermeasures effectiveness. The system then alerts the smart countermeasures dispenser to release the appropriate number and type of flares. ATIRCM uses both laser and xenon lamp technology. A key advantage of the ATIRCM architecture, according to Colonel Reinkober is that "everything is automatic. There is no pilot load (or involvement)". ATIRCM is drawing near to the engineering and manufacturing development phase (EMD).

The ATRJ system, also nearing EMD, handles the radio frequency (RF) end of the threat environment. According to Colonel Reinkober, "ATRJ will combine radio frequency interference (RFI), radar warning and jamming in a single package that provides 360 degree coverage. Both pulse and CW jamming will be delivered." ATRJ architecture brings significant weight savings over previous systems. The ATRJ and ATIRCM systems will be capable of interoperation. One point of connectivity is the smart dispenser, shared jointly when both systems are installed in the same platform.

Colonel Reinkober's office, working with support contractors, developed an unclassified electronic bulletin board which readily provides EW information to the field. This bulletin board, up and running, contains EW maintenance reports, threat data, logistics information, safety bulletins and other important data to keep field users updated on the changing world of ASE. It currently has only one-line access to the data base, but plans call for addition of up to seven more lines in the next few months.

Colonel Reinkober has also provided initiatives in several categories under the Army's Digital Battlefield concept. These include the Improved Data Modem, which enhances communication capabilities with platforms from other services, and the Aviation Mission Planning Station

(AMPS) which enables operators to upload mission data directly into the helicopter's mission computers.

His new post is the deputy program executive officer for Foreign Military Sales (FMS) under the program executive officer for aviation. Meanwhile, the hallmarks of the Army's next generation of EW systems - commonality across platforms and integrated architectures and functionality - will remain as a testament to his art as the Army EW renaissance continues.

Colonel Reinkober has been one of the strongest ARAT supporters over the past few years. The ARAT community will greatly miss his innovative ideas, leadership and support. His vision and foresight have ensured that ARAT becomes a key element of Army EW. POCs are Mr. Sok Kim/Mr. Ray Johnson, DSN: 992-1337.

---

## ARAT BBS: THE E-MAIL OPTION (Part 2 in a Series)

*"Communications dominate the war; broadly considered, they are the most important single element in strategy, political or military".*

*Mahan: The Problem of Asia, 1900*

Part 1, (ARAT BULLETIN, July 1994), introduced the ARAT BBS and provided a general overview. Part 2 discusses the E-mail option.

The Bulletin Board System (BBS) Electronic Mail (E-mail) option provides users with the capability to send and receive mail, classified and unclassified, electronically. This is a primary method for the Army Reprogramming Analysis Team - Threat Analysis (ARAT-TA) to communicate and send files to field users, responsible centers, and agencies. BBS users typically include the various software engineering centers, threat analysis centers, program managers, TRADOC, major commands and other agencies involved with the reprogramming process.

You can send text data such as tactics, techniques, threat information, and reprogrammable binary data via E-mail. Messages may include an attached data file, which is viewed on line or downloaded onto a hard drive or floppy disk for later viewing. Data transfers may be classified or

**(continued on Page 7)**

## ARAT BBS: E-MAIL (continued)

unclassified and must be handled accordingly.

After logging onto the BBS, you see the BBS Main Menu. You use the E-mail option by pressing "E" from this menu. The E-mail menu is now displayed (see figure below). Each letter initiates a particular function.

You can start the receipt of mail by pressing "R". You can display the header message or the entire message on your monitor.



When sending a message, you type the name of the person or agency for an address. If the BBS doesn't recognize the name, it provides you with a list of candidates from which to choose. The BBS also has a Register User Identification option that provides specific user information. This option is accessed from the BBS Main Menu.

E-mail can communicate with one or more specific users. A user list is provided in the BBS user registry. If messages are available when you first log onto the BBS, you will be prompted to read them. You can read them any time during your BBS session. Other services accessed from the E-mail menu let you perform special functions, modify messages, and erase information.

**ATRR-PO personnel can now access the classified BBS through their PCs.**



This overview shows that use of the BBS E-mail option can enhance the reprogramming process. More details are available while on-line and in the BBS User manual. Future articles on the BBS will address downloading/uploading files and protocols. POCs are Mr. Norm Svarrer, DSN: 872-8899/Mr. Tony Munoz, DSN: 992-1337.

## EDITOR'S NOTE

LTC Bert Napoleon, Officer-In-Charge (OIC) of the ARAT Threat Analysis Center, has temporarily departed this duty for special assignment with the U.S. Army forces restoring peace, hope, and democracy in Haiti. Hand-selected by the Department of Army Staff, we understand that Bert is providing liaison services between US and Haitian military and political leaders. We are all confident that his background and experience will prove to be invaluable to military commanders in Haiti. We want to send Bert and his family our best wishes for a speedy and safe return home.

ARAT Community

## Pump Up the Volume- Here Comes the Jams! by Zachary A. Lum

*The following article is an excerpt from the original story, published in Journal of Electronic Defense, June 1994. Reprinted by permission of the Journal of Electronic Defense, Horizon House Publications, Inc. The Journal of Electronic Defense is the official publication of the Association of Old Crows.*

Communications technology is seeing constant, dynamic progress which includes such areas as frequency hopping and spread- or swept-spectrum techniques. Unfortunately for United States counter-command and control warfighters, these advances have not remained confined to the protected labs and research centers of the U.S. government. Russia has been actively marketing its advanced radios, along with its weapons and airplanes, around the world. Other countries are doing the same thing. The multiplicity of advanced communications systems sold presents a complex picture for the U.S. military.

(continued on Page 8)



---

## Turn Up The Jams (continued)

In response to these developments, the Air Force and Army are either upgrading or developing some high-profile electronic-attack (EA) systems for the next battleground. According to an industry official, there is always the hard kill option where you "shoot a missile at the transmitter" which was successfully used in Desert Storm. Or you can put up an airplane that throws out 20 billion watts of energy.

Among all the services, there currently exists only one deep-coverage C2W countermeasures asset capable of delivering a jamming payload of this magnitude - the Air Force's Compass Call. Compass Call employs a number of high-power communications and radar jammers, abetted by advanced computer-controlled receivers, to conduct command and control warfare (C2W) and non-lethal suppression of enemy air defenses (SEAD) from behind the relative safety of the forward line of own troops (FLOT).

Other C2W jammers exist which fly lower and possibly closer to the action. The Army has the EH-60A Advanced Quickfix helicopter, the airborne element in the service's triptych of Intelligence and Electronic Warfare Common Sensor (IEWCS) platforms. On the ground, the IEWCS subsystems will be carried by the HMMWV and the Bradley Fighting Vehicle, the same platforms used by the divisions which Common Sensor will support. There is a high degree of interoperability among these platforms. Now, the Air force is exploring the possibility of linking Compass Call to this Army network.



**HMMWV with the IEWCS platform**  
(photo reprinted courtesy of Journal of Electronic Defense)

IEWC has a potent weapon to conduct C2W EA - the TACJAM-A which is a next generation EW system. TACJAM-A incorporates both Electronic Support (ES) and EA in one suite, employing "smart" jamming techniques to address modern modulations that current systems cannot. Like all the Common Sensor subsystems, the TACJAM-A is modular in nature, and thus explicitly designed to accommodate future upgrades to counter evolving communications technology.

Notwithstanding the current proliferation of more advanced communications technology, another post-Cold War issue has reared its head to affect the way the US military approaches C2W. According to a senior Marine official, while EA is an undoubted force multiplier in large-scale, head-to-head warfare, in the scenarios projected for the foreseeable future - characterized by low-intensity conflict, limited objectives and anti-

terrorist operations - restraint may become the wisest tactic. "We would expect to find less of that ECM because of the value of the ESM. The value of the information far outweighs the suppression of the information." While the high-value EA assets of Compass Call and IEWCS will certainly retain their significance in the force structure, perhaps their most useful function will be to hear, but not be heard.

The ARAT community is confident that the Army will include provisions for rapid reprogramming into the designs of these and future Target Sensing Systems (TSS). Such foresight will ensure that any and all EW challenges can be overcome. POCs are Mr. Sok Kim/Mr. Ray Johnson, DSN: 992-1337.

---

### ...MEET THE ARAT BULLETIN STAFF...

#### **Publishers:**

**Cenap Dada, Chief, A/IEW**  
**John Hakim, Chief, CM**

#### **Executive Editor:**

**Sok Kim, ATRR-PO**

#### **Editor:**

**Ray Johnson**

#### **Assistant Editor:**

**Jackie Yamello**

---

**To receive this publication, submit the following:**

- \* **Organization**
- \* **POC**
- \* **Address**
- \* **Phone #/Fax #**

#### **Fax to:**

**(908) 532-5238 (U)**

#### **or send via Email to:**

**arat@ccmail.sed.monmouth.army.mil**